ANASTACIA has received funding from the European Union's **Horizon 2020 Research and Innovation Programme** under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

2nd ECSCI Workshop

Stefano Bianchi
algoWatt SpA

April 27th 2022

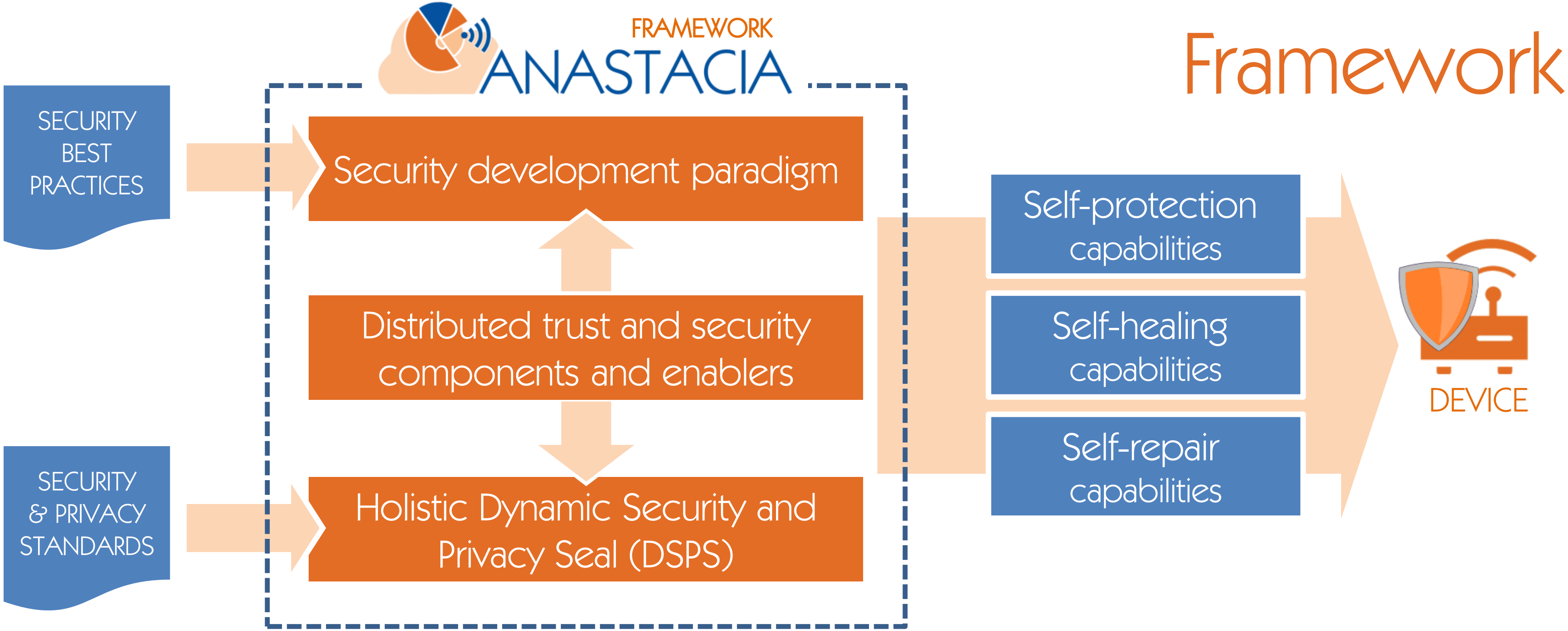
ANASTACIA
CYBERSANE
CyberSEAS
DEFENDER
FINSEC
ENSURESEC
INFRA STRESS
ENERGY SHIELD
FeatureCloud
SAFECARE
PHOENIX
SOTER
IMPETUS
SMART RESILIENCE
SATIE
STOP-IT
7SHIELD
RESISTO
Sealed GRID
SecureGas
SPHINX
PRECINCT
EU-HYBNET
PRAETORIAN
EUROPEAN CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES
SCIENTIFIC COLLABORATION
TECHNICAL COLLABORATION
COMMUNICATION & DISSEMINATION
STAKEHOLDERS' ALLIANCE
MARKETPLACE
SALE

This presentation only reflects the Consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

Motivation

- Cyber-attacks on IoT are getting more and more widespread, due to:
  - Dynamically evolving nature of systems
  - Increased internet-connectivity of equipment
  - Constrained capabilities of IoT systems, misconfigurations, absence of software updates, etc.
  - Lack of interoperability of devices deployed on distributed smart IoT deployments.
- Thereby, new types of attacks and 0-day vulnerabilities, such as Slow DoS Attacks (SDA), are emerging and evolving
- However, current network security solutions monitoring, management and reaction systems/tools present low responsiveness and can unlikely cope with the dynamic IoT environments
  - Besides, the deployment and management of NSFs (Network Security Functions) to mitigate cyber-attacks have not yet properly studied and exploited in NFV/SDN-enabled IoT networks.
- All these security vectors claim for new context-aware security frameworks to allow orchestrating NFV managers, SDN controllers and IoT controllers across IoT domains, thereby providing security chaining, as well as dynamic reconfiguration and adaptation of the virtual security appliances according to monitoring and reaction mechanisms.

Framework


FRAMEWORK
ANASTACIA
SECURITY BEST PRACTICES
SECURITY & PRIVACY STANDARDS
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
DEVICE

To develop a autonomic security framework able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools

General Use Case

Hetereogenous and distributed Smart IoT Deployments,
facing evolving kind of cyber-attacks

Enterprise
Networkings
Helth, Banks,
Medical systems
Smart Industry
Metropolitan
Networks
Smart Parking
Community Networks
Smart Buildings
Mangement Systems
Smart Home
Smart Cities

April 27th 2022

Reference scenario

- ANASTACIA addresses the security management of distributed IoT scenarios, such as Smart Buildings or Smart Cities, that can benefit from policy-based orchestration and management approach, NFV/SDN-based solutions and novel monitoring and reaction tools to cope with new kind of cyber-attacks
- Security VNFs can be timely and dynamically orchestrated through policies to deal with heterogeneity demanded by these distributed IoT deployments, than can be deployed either at the core of at the edge, in VNF entities, in order to rule the security in IoT networks
- Dynamic and reactive provisioning of security VNFs towards the edge of the network can enhance scalability, necessary to deal with IoT scenarios
- Dealing with this general problem statement and use case raises several research challenges, being faced in ANASTACIA

Research Challenges

- Interoperable and scalable IoT security management
  - Security policies to deal with IoT heterogeneity and interoperability across IoT domains
  - Challenges:
    - Dealing with the level of abstraction, the language and new security models.
    - contextual IoT aspects in policies,
    - particularities in IoT security models,
    - policy conflicts and dependencies in orchestration policies

- Optimal selection of SDN/NFV-based security mechanisms
  - Using the virtualization enabled by SDN and NFV allows a quick instantiation of VMs in the adequate location to overcome traditional hardware-based deployment.
  - This lack of elasticity can be easily handled by VNF functions that we can chain and place on-demand according to the attacks.
  - Challenge: **allocate multiple VNF requests on an NFV Infrastructure,** especially in a cost-driven objective.
    - Depending on their type and isolation considerations, VNFs can be potentially shared among several Service Function Channings (SFC)
    - VNFs must not be placed far from the shortest path to avoid increasing delay and network usage.

Research Challenges

- Orchestration of SDN/NFV-based security solutions for IoT environments
  - Challenges:
    - The **selection of the adequate mitigation plan** and the fast enforcement of the defined policies
    - **Orchestration and the enforcement** of the adequate countermeasures in a short time, and without affecting (QoS)
    - Definition and enforcement of **mitigation plans** *while* **reducing** the deployment **cost** and by taking into account the limitations in existing infrastructure clouds.

- Dealing with new kind of cyber-attacks in IoT
  - The identification and consequent protection from novel attacks exploiting Internet of Things networks and sensors
  - Challenge: to provide advanced security from **last generation threats** on IoT environments.

Research Challenges

- Learning Decision Model for Detecting Malicious Activities
  - continued **rise of cyber-attacks** together with the evolving skills of the attackers
  - **inefficiency** of the traditional security algorithms to defend against advanced and sophisticated attacks such as DDoS, slow DoS and zero-day
  - Challenge: the development of **novel defense and resilient detection techniques**
    - New decision models needed → learning a set of constraints/relations from the data to learn normal operations and communication flows

- Hybrid Security Monitoring for IoT enhanced with event correlation
  - The application of both **signature-based** and **behavioural-based** security analysis for IoT networks provides an initial security level.
  - Challenge: correlating both types of events to **detect hidden relations** and thus identify potential threats

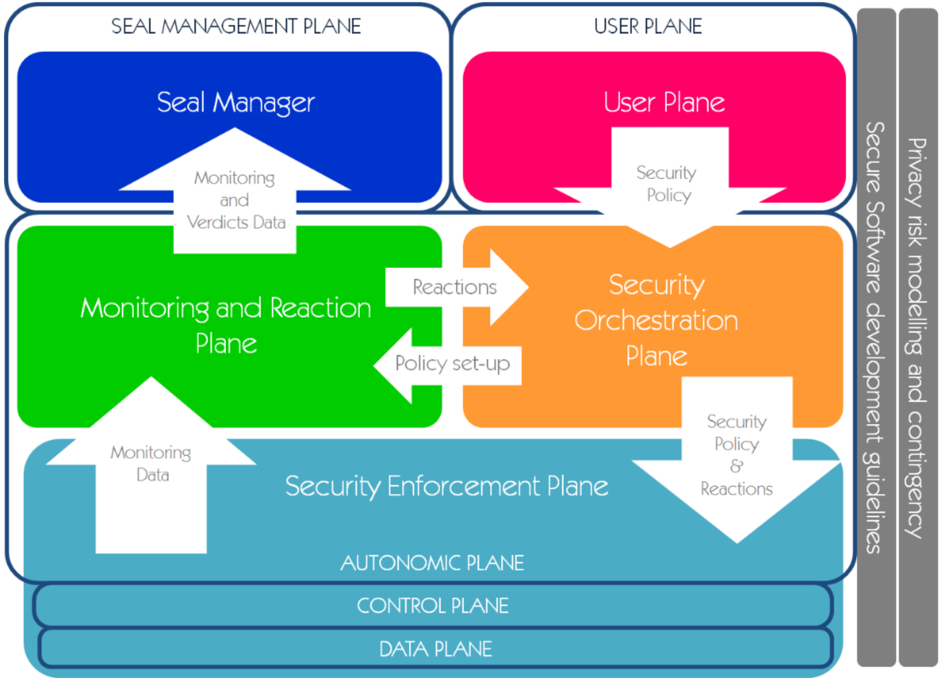
Research Challenges

- Quantitative evaluation of incidents for mitigation support
  - Challenge: combination of several factors to evaluate incidents to decide on the most **convenient mitigation plan** to enforce, including
    - Incident severity
    - Criticality of assets affected
    - Global risk associated to the incident
    - Cost of potential mitigations

- Developing a Dynamic Security and Privacy Seal which secures both organizational and technical data
  - Generate trust by considering
    - Technical insights on security and privacy
    - Personal data protection requirements that might be of relevance to the organization
  - Challenge: integrate the end-user (CISO and DPO) in the seal creation process
    - Seal to generate non-repudiable, legally valid proof of due-diligence and compliance with Legal or contractual requirements

ANASTACIA's Approach

- To cope with those challenges Anastacia is designing, implementing and evaluating a holistic and dynamic SDN/NFV-based Security framework for IoT


SEAL MANAGEMENT PLANE
USER PLANE
Seal Manager
User Plane
Monitoring and Verdicts Data
Security Policy
Monitoring and Reaction Plane
Reactions
Policy set-up
Security Orchestration Plane
Monitoring Data
Security Enforcement Plane
Security Policy & Reactions
AUTONOMIC PLANE
CONTROL PLANE
DATA PLANE
Secure Software development guidelines
Privacy risk modelling and contingency

ANASTACIA's main Key Innovations(KI)

1. Holistic policy-based security management and orchestration in IoT
2. Investigation on innovative cyber-threats
3. Trusted Security orchestration in SDN/NFV-enabled IoT scenarios
4. Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies
5. Security monitoring to threat detection in SDN/NFV-enabled IoT deployments
6. Cyber threats automated and cognitive reaction and mitigation components
7. Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments
8. Secured and Authenticated Dynamic Seal System as a Service

ANASTACIA's main Key Innovations(KI)

1. Holistic policy-based security management and orchestration in IoT:
   - **New Security Models (including IoT aspects):** Authentication, Authorization, Traffic Divert, Filtering, Channel Protection, Operation, Monitoring, **IoT management, IoT Honeynet,** Privacy, QoS, Data Aggregation, Policy for Orchestration, Anonymity
   - **Policy Conflict Detection** engine verifies that the new security policy will not generate conflicts like redundancy, priorities, duties
   - **Policy for Orchestration** model allows the security administrator to specify how a set of security policies must be enforced by defining priorities and dependencies
2. Investigation on innovative cyber-threats
   - **IoT 0-Day attack** investigating the domotic IoT context and exploiting its components, in order to identify weaknesses that attackers may exploit.
   - **Slow DoS Attacks**: concerns a DoS attack which makes use of low-bandwidth rate to accomplish its purpose
3. Trusted Security orchestration in SDN/NFV-enabled IoT scenarios
   - **Orchestration** of SDN/NFV-based security solutions for IoT environments
     - **IoT controller**: It provides IoT command and control at high-level of abstraction in independent way of the underlying technologies
     - **NFV orchestrator**: integrated SDN controller (ONOS) with the used Virtual Infrastructure Manager (VIM),
     - **SDN controller**: The security orchestrator should push the adequate SDN rules to reroute the traffic between different VNFs in the SFC and the IoT domain.
   - Currently several **research experiments** have been carried out in different security areas
     - **Virtual IoT-honeynets, vAAA, vChannelProtection, vFirewall**
   - Trusted cloud platform to **prevent VNF manipulation**

ANASTACIA's main Key Innovations(KI)

4. Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies
   - Selection of best VNF "**The security enablers selection**"
     - Minimize the maximum load nodes, considering server capacity (CPU, RAM, etc), and VNF flavours (CPU, RAM, etc)…
   - **Security Enabler Provider**: provides candidates from the main identified capabilities
   - Dynamic Service Function Chain (**SFC**) requests placement that aim to reduce the routing overhead in case of an attack happen
   - **Graph-based algorithm** that, taking into account a maximum MEC server capacity, provides a partition of MEC clusters, which consolidates as many communications as possible at the edge.
5. Security monitoring to threat detection in SDN/NFV-enabled IoT deployments
   - Holistic monitoring and reaction framework
   - Monitoring Agents:
     - NFV- and SDN-based monitoring agents
     - Monitoring Agents adapted for IoT networks
   - Enhanced engine for reaction computation (VDSS)
     - Risk analysis-based computation
   - Monitoring algorithms for slow DoS attacks
   - Events correlation engine, relationships between events and possible attacks

ANASTACIA's main Key Innovations(KI)

6. Cyber threats automated and cognitive reaction and mitigation components
   - Quantitative model to automatically analyze several factors and, along with the incidents detected, evaluates and decides on the most convenient mitigation in each case
     - Severity of the incidents
     - Importance of the assets affected
     - The cost of the mitigation
   - Decision support service (DSS) is used to compute that information, providing with a score for each mitigation
7. Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments
   - Behavioral framework automatically identifies cyber-security attacks in a given IoT environment
   - Prediction of potential security consequences of interacting operations among subsystems and generate threat alarms
   - Constraint Programming (CP) model, continuous stream of data (i.e. time-series) aggregating and modeling the normal behaviour of the system
   - CP-model provides explanation when a potential anomaly is detected

ANASTACIA's main Key Innovations (KI)

8. Secured and Authenticated Dynamic Seal System as a Service

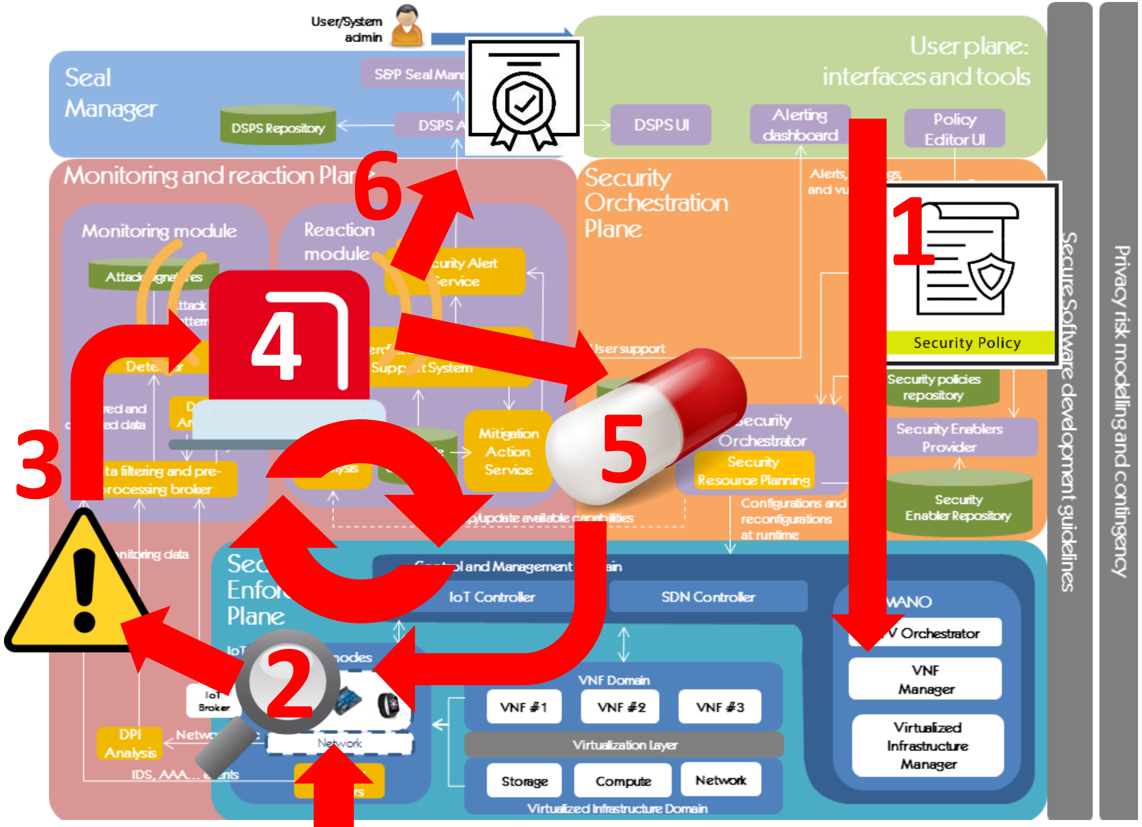
- **Inform the end-user** on the most relevant privacy and security issues while supporting certification and compliance activities.
- **DSPS Combining**
  - The certainty and trustworthiness of conventional certification schemes
  - Real-time certification surveillance capabilities through the real time dynamic monitoring
- Compile alerts and threats from ANASTACIA, compatible monitoring solutions (using the STIX 2 standard) and the end-user (CISO/DPO) and showcase them through a **unified GUI**
- enabling the client's (DPO) and (CISO) to **provide feedback to the raised alerts** directly through the GUI

ANASTACIA architecture

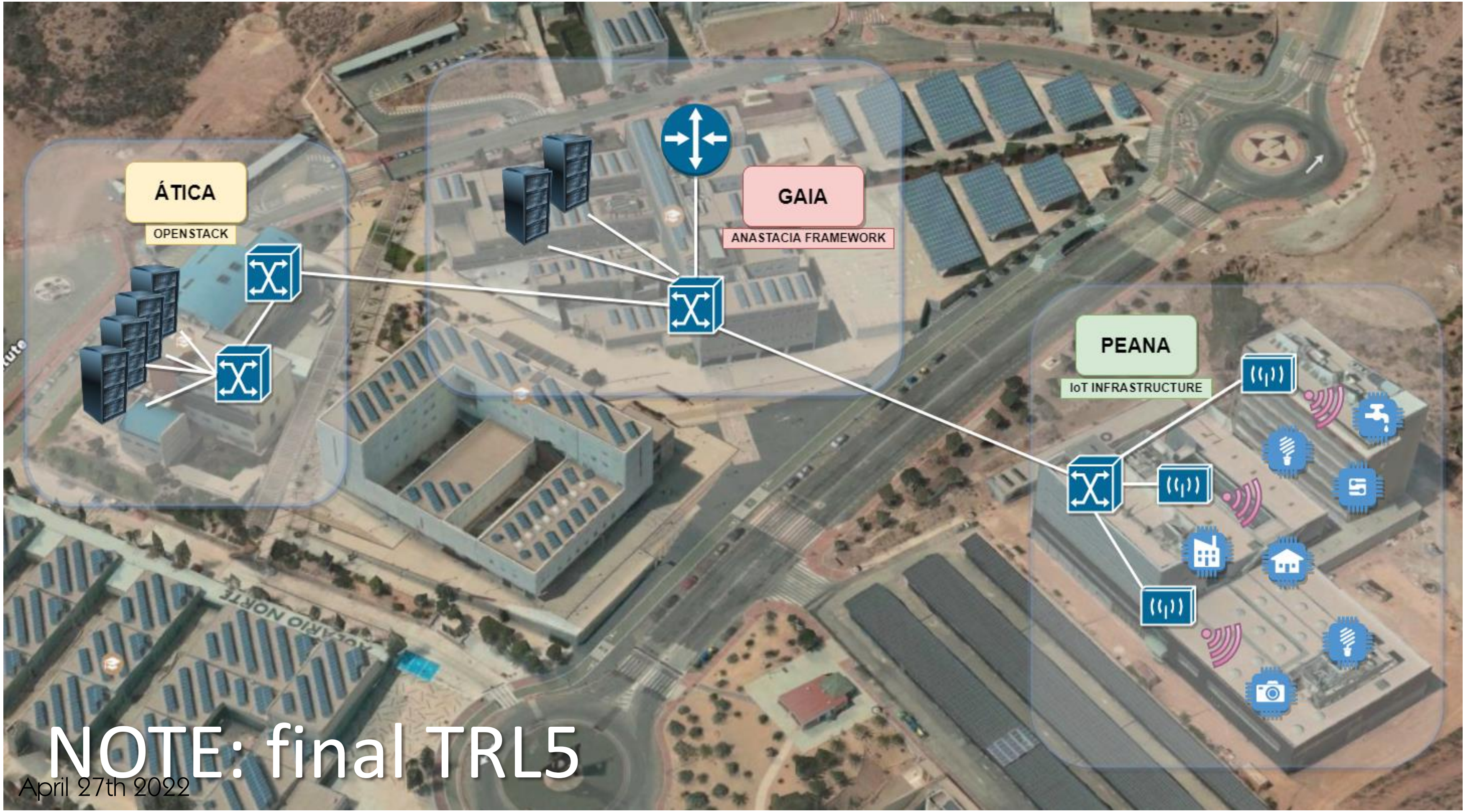
1. Policy setup

   Attack

2. Monitoring
3. Probes detection
4. Incidents detected
5. Countermeasures enforcement
6. S&P Seal evaluation



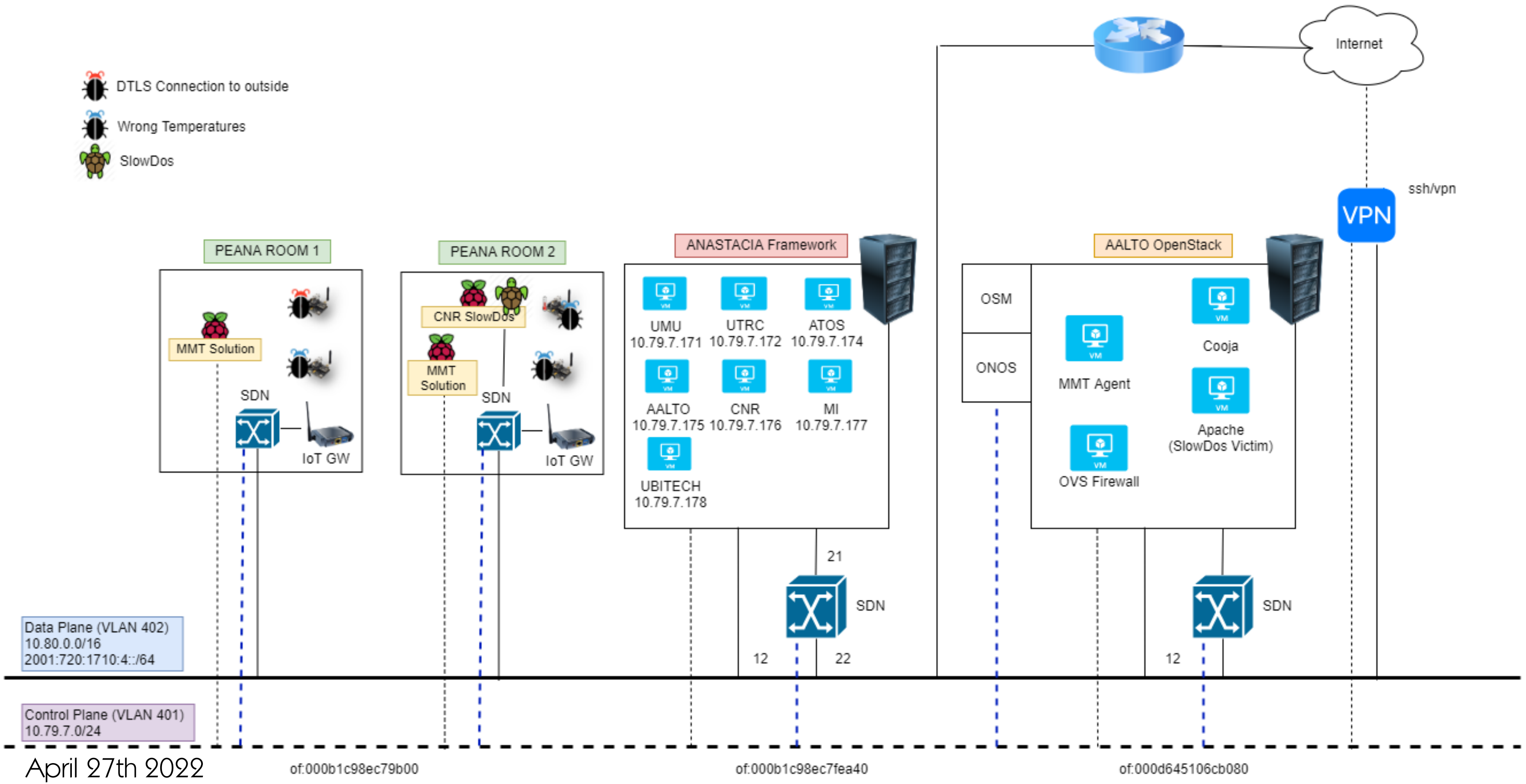
UMU Final Demo Premises



NOTE: final TRL5

April 27th 2022

UMU Final Demo Deployment



DTLS Connection to outside

Wrong Temperatures

SlowDos

PEANA ROOM 1

MMT Solution

SDN

IoT GW

PEANA ROOM 2

CNR SlowDos

MMT Solution

SDN

IoT GW

ANASTACIA Framework

UMU 10.79.7.171

UTRC 10.79.7.172

ATOS 10.79.7.174

AALTO 10.79.7.175

CNR 10.79.7.176

MI 10.79.7.177

UBITECH 10.79.7.178

21

SDN

12

22

Internet

ssh/vpn

VPN

AALTO OpenStack

OSM

ONOS

MMT Agent

Cooja

Apache (SlowDos Victim)

OVS Firewall

SDN

12

Data Plane (VLAN 402)
10.80.0.0/16
2001:720:1710:4::/64

Control Plane (VLAN 401)
10.79.7.0/24

of:000b1c98ec79b00

of:000b1c98ec7fea40

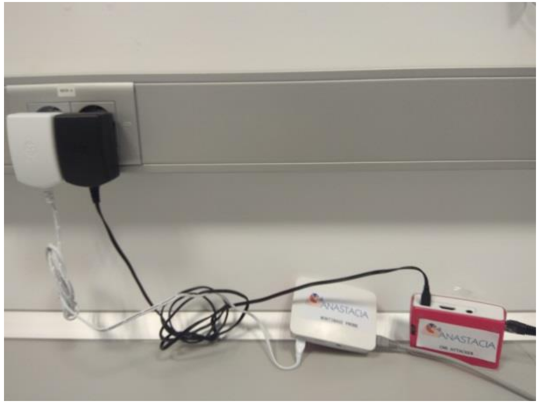
of:000d645106cb080

April 27th 2022

Demo Equipment for Smart Building

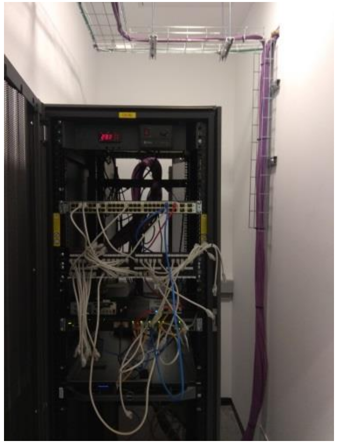
- PEANA Experimental Labs
- Smart Lighting
- Energy Efficiency & HVAC
- Fire Alarm Devices
- Environment Sensors
- Gases Sensors (CO2, Tolueno)
- RFID Access Control

- Temperature Sensors
- DTLS+COAP Attackers
- 6LowPAN Bridge



- MMT Monitoring Probes
- CNR SlowDoS attackers

Demo Equipment for Smart Building

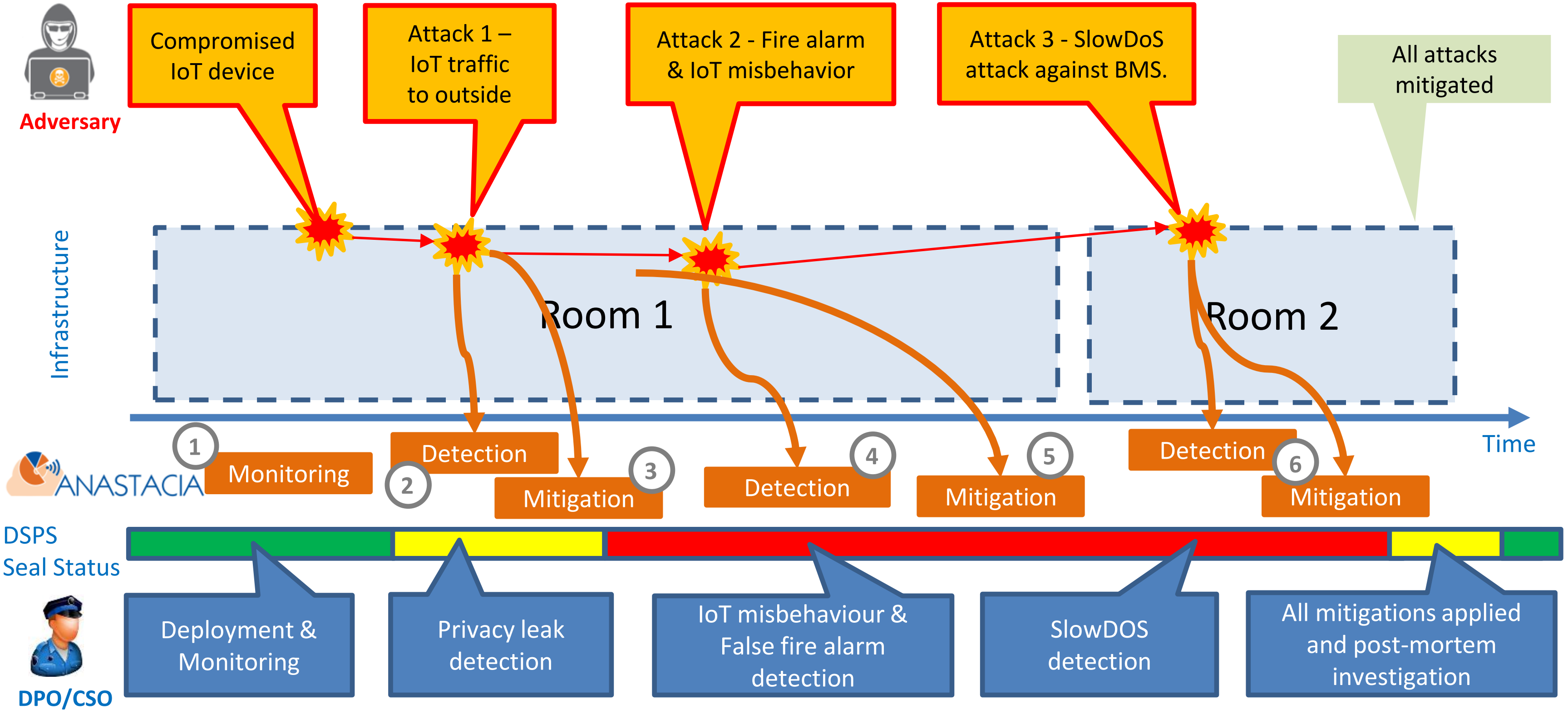


- SDN switches
- NFV infrastructure
- Data/Control Planes

- Fake ceiling for Network & Energy
- Experimental Scenario with IoT sensors and actuators

- Wireless network (6lowpan & Wifi)
- Ethernet network

DEMO STORYBOARD



Adversary

Compromised IoT device

Attack 1 – IoT traffic to outside

Attack 2 - Fire alarm & IoT misbehavior

Attack 3 - SlowDoS attack against BMS.

All attacks mitigated

Infrastructure

Room 1

Room 2

Time

ANASTACIA

1 Monitoring

2 Detection

3 Mitigation

4 Detection

5 Mitigation

6 Detection

Mitigation

DSPS Seal Status

DPO/CSO

Deployment & Monitoring

Privacy leak detection

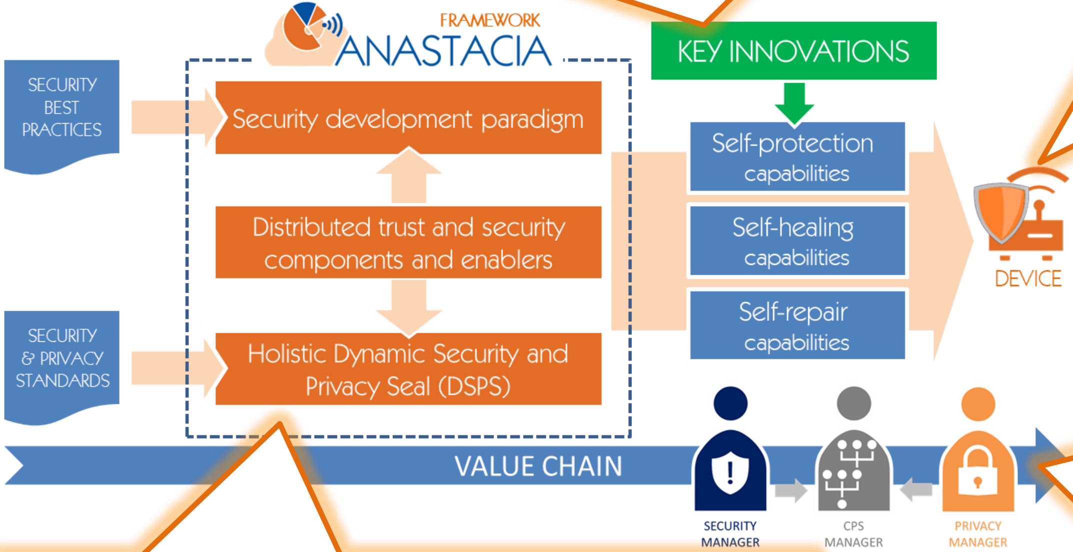
IoT misbehaviour & False fire alarm detection

SlowDOS detection

All mitigations applied and post-mortem investigation

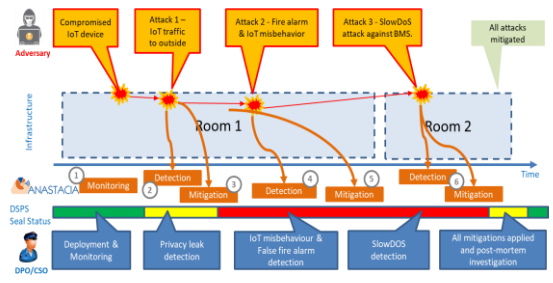
In a nutshell…

Research & Innovation Action
releasing a fully integrated modular framework
based on significant technological advancements &
a complete actionable Proof-of-Concept (PoC)


ANASTACIA
FRAMEWORK
SECURITY BEST PRACTICES
SECURITY & PRIVACY STANDARDS
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
KEY INNOVATIONS
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
DEVICE
VALUE CHAIN
SECURITY MANAGER
CPS MANAGER
PRIVACY MANAGER

TRL 5 – technology validated in relevant environment (UMU premises)

Challenging complex DEMO Use Case



Key Innovation-based Key Exploitable Assets
identified with individual/joint exploitation
plans in place & on-going collaborations

ANASTACIA

ANASTACIA

algoWATT GREEN TECH SOLUTIONS

THALES

Atos

ERICSSON

United Technologies Research Center

UBITECH ubiquitous solutions

montimage

MANDAT INTERNATIONAL

OdinS

UDG UNIVERSAL DEVICE GATEWAY

Consiglio Nazionale delle Ricerche

A! Aalto University

UNIVERSIDAD DE MURCIA

ANASTACIA has received funding from the European Union's
Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558
and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA has received funding from the European Union's **Horizon 2020 Research and Innovation Programme** under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

http://www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

TYPE:	Research & Innovation Action
CALL:	H2020-DS-LEIT-2016
TOPIC:	DS-01-2016 Assurance and Certification for Trustworthy and Secure ICT systems, services and components
DURATION:	36 MONTHS (Jan 2017 → Dec 2019)
COSTS:	€ 5,420,208.75
FUNDING:	€ 3,999,208.75
G.A.:	731558